BÁO CÁO BÀI THỰC HÀNH SỐ 2

PHÂN TÍCH MỘT SỐ KỸ THUẬT TẤN CÔNG TRONG MẠNG LAN

***Sinh viên 1:***

***Sinh viên 2:***

***Yêu cầu kết quả thực hành:***

Đóng gói các kết quả vào file nén có tên theo định dạng NhomX\_Lab02\_BaoCao.zip

* Báo cáo kết quả thực hành
* File bắt lưu lượng của mỗi kịch bản. Kích thước mỗi file không quá 1 MB.

**KẾT QUẢ THỰC HÀNH**

Thông số của các container trước khi thực hiện tấn công **(1 điểm)**

* Máy User:
* Địa chỉ IP:
* Địa chỉ MAC:
* Bảng ánh xạ ARP

*<Ảnh chụp màn hình kết quả>*

* Máy Server:
* Địa chỉ IP:
* Địa chỉ MAC:
* Bảng ánh xạ ARP

*<Ảnh chụp màn hình kết quả>*

* Máy Attacker:
* Địa chỉ IP:
* Địa chỉ MAC:

1. **Kịch bản 1 (2 điểm)**

Phân tích lưu lượng tấn công và kết quả quan sát được để trả lời các câu hỏi sau:

* Tìm gói tin mà máy tấn công đã gửi đi để thực hiện tấn công ARP Cache Poisoning. ***(1 điểm)***

*<Ảnh chụp màn hình thể hiện gói tin trên giao diện của Wireshark >*

* Số thứ tự (No.):
* Địa chỉ nguồn:
* Địa chỉ đích:
* Loại gói tin là ARP Request hay ARP Reply?
* Đặc điểm khác thường của gói tin này so với thông tin thực tế của mạng là gì?
* Theo các thông tin đã phân tích từ trên, máy nào đã bị tấn công? Hậu quả của tấn công trên máy nạn nhân là gì? ***(1 điểm)***

*<Ảnh chụp màn hình máy nạn nhân để minh chứng hậu quả>*

1. **Kịch bản 2 (2 điểm)**

Phân tích lưu lượng tấn công và kết quả quan sát được để trả lời các câu hỏi sau:

* Tìm gói tin mà máy tấn công đã gửi đi để thực hiện tấn công ARP Cache Poisoning. ***(1 điểm)***

*<Ảnh chụp màn hình thể hiện gói tin trên giao diện của Wireshark >*

* Số thứ tự (No.):
* Địa chỉ nguồn:
* Địa chỉ đích:
* Loại gói tin là ARP Request hay ARP Reply?
* Đặc điểm khác thường của gói tin này so với thông tin thực tế của mạng là gì?
* Theo các thông tin đã phân tích từ trên, máy nào đã bị tấn công? Hậu quả của tấn công trên máy nạn nhân là gì?***(1 điểm)***

*<Ảnh chụp màn hình máy nạn nhân để minh chứng hậu quả>*

1. **Kịch bản 3 (3 điểm)**

Phân tích lưu lượng tấn công và kết quả quan sát được để trả lời các câu hỏi sau:

* Tìm các gói tin mà máy tấn công đã gửi đi để thực hiện tấn công ARP Cache Poisoning.***(1 điểm)***

*<Ảnh chụp màn hình thể hiện gói tin trên giao diện của Wireshark >*

* Hậu quả của tấn công trên máy nạn nhân là gì? ***(1 điểm)***

*<Ảnh chụp màn hình máy nạn nhân để minh chứng hậu quả>*

* Thông điệp mà máy Server nhận được có gì thay đổi so với trước khi bị tấn công? Giải thích tại sao có sự thay đổi này?***(1 điểm)***
* Trước khi bị tấn công

*<Ảnh chụp màn hình thể hiện gói tin chứa thông điệp mà User gửi>*

*<Ảnh chụp màn hình thể hiện gói tin chứa thông điệp mà Server nhận>*

* Sau khi bị tấn công

*<Ảnh chụp màn hình thể hiện gói tin chứa thông điệp mà User gửi>*

*<Ảnh chụp màn hình thể hiện gói tin chứa thông điệp mà Server nhận>*

* Nhận xét thay đổi

1. **Phòng chống tấn công (2 điểm)**

* Lệnh định nghĩa ánh xạ ARP cố định đã thực hiện trên máy User là gì? ***(0.5 điểm)***

*<Ảnh chụp màn hình thực hiện lệnh trên máy User>*

* Kết quả tấn công là gì? Hãy giải thích? ***(1.5 điểm)***

*<Ảnh chụp thể hiện kết quả tấn công>*